

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY

JOSEPH OAT HOLDINGS, INC.,  
BIOTHANE CORPORATION, ROBERT  
SAX, MICHAEL HOLTZ, GRAIG  
ROSENBERGER, MARTIN KAPLAN,  
RONALD KAPLAN, JOHN MURPHY,  
AND RCM BIOTHANE, LLC,  
Plaintiffs,

v.

RCM DIGESTERS, INC. AND MARK  
MOSEY,  
Defendants/ Counterclaimants/  
Third-Party Plaintiffs.

CIVIL NO. 06-4449 (NLH) (JS)

**OPINION**

**APPEARANCES:**

Richard J. Kravitz, Esquire  
Mukti Naresh Patel, Esquire  
Patricia C. McManus, Esquire  
Fox Rothschild, LLP  
Princeton Pike Corporate Center, Building 3  
997 Lenox Drive  
Lawrenceville, NJ 08648-2311  
*Attorneys for Plaintiffs*

William J. DeSantis, Esquire  
Joseph Kenney, Esquire  
Ballad Spahr Andrews & Ingersoll, LLP  
Plaza 1000 - Main Street  
Suite 500  
Voorhees, NJ 08043

James C. Duda, Esquire  
Eric D. Beal, Esquire  
Bulkley, Richardson and Gelinas, LLP  
1500 Main Street, Suite 2700  
Springfield, MA 01115  
*Attorneys for Defendants/Counterclaimants/Third-Party  
Plaintiffs*

**HILLMAN**, District Judge

Plaintiffs Joseph Oat Holdings, Inc. ("JOHI"), Biothane  
Corporation ("Biothane"), Robert Sax, Michael Holtz, Graig

Rosenberger, Martin Kaplan, Ronald Kaplan, John Murphy, and RCM Biothane filed a Verified Complaint consisting of eight claims against Defendants RCM Digesters, Inc. ("RCM Digesters") and Mark Moser. Defendants filed an answer, a verified counterclaim consisting of 29 counts, and a third-party complaint<sup>1</sup> consisting of two counts. On March 31, 2009, this Court denied plaintiffs' motion for summary judgment on ten counts in defendants' counterclaim and both counts of the third-party complaint. Now before the Court are plaintiffs' and defendants' motions for partial summary judgment on defendants' counterclaims regarding plaintiffs' copying of defendants' computer files. For the reasons expressed below, plaintiffs' motion will be denied, and defendants' motion will be granted in part and denied in part.

#### **BACKGROUND & DISCUSSION**

Moser was the founding stockholder of RCM Digesters, a business that promoted, designed, built, and sold anaerobic digester systems.<sup>2</sup> Contemporaneously, Biothane existed as a multinational corporation specializing in the biological treatment of industrial wastewater. As a result of a series of agreements between the parties, Biothane's principals and Moser (who was RCM

---

<sup>1</sup>The third-party complaint is asserted against JOHI; the counterclaims are asserted against JOHI, Biothane and/or the individual defendants.

<sup>2</sup>Anaerobic digestion systems are vessels containing bacteria that break down organic wastes, such as manure, without air, and produce methane as a byproduct.

Digesters' principal) created RCM Biothane pursuant to a Certificate of Formation dated February 17, 2005. JOHI was to own 80% of RCM Biothane, and Moser was to own 20%.

A year and a half later, due to what plaintiffs call a "stormy relationship," the parties agreed to terminate the operation of RCM Biothane. On August 7, 2006, the parties entered into a separation agreement (the "Separation Agreement"), which was signed by the six individual plaintiffs and Moser. At that point RCM Biothane ceased to exist, and the two entities reverted back to their original independent status as Biothane Corp. and RCM Digesters.<sup>3</sup>

The main issue in this case,<sup>4</sup> which constitutes more than 40 counts of alleged violative conduct by the parties, is the validity of the Separation Agreement and its effect on the parties' prior agreements and duties going forward. In the Court's March 31, 2009 Opinion, summary judgment as to the validity of the Separation Agreement was denied, and all claims concerning that agreement, including defendants' claims of breach of fiduciary duty, unjust enrichment, libel, and intentional infliction of emotional distress, are proceeding to a trial by jury.

The current issue before the Court is plaintiffs' copying and

---

<sup>3</sup>As discussed in the Court's March 31, 2009 Opinion, the parties dispute Moser's conduct following the August 7, 2006 dissolution of RCM Biothane and the winding down of its affairs.

<sup>4</sup>This Court has jurisdiction over the federal claims under 28 U.S.C. § 1331, and supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

alleged destruction of defendants' computer files after August 7, 2006, the date of the Separation Agreement and the date both sides agree marked the end of their joint venture. When RCM Biothane was formed in April 2005, defendants' computers in Oakland, California were connected to plaintiff JOHI's computer system through a virtual private network (VPN). All of defendants' files continued to reside on the Oakland "cube" server, but JOHI had access to those files through the VPN. After the parties agreed to dissolve RCM Biothane, and even after plaintiffs filed their complaint against defendants on September 20, 2006 and obtained a TRO which enforced the dissolution, the parties' computers were still connected via the VPN, despite the fact that the computer system in Oakland reverted back to RCM Digesters. As reflected in the Separation Agreement<sup>5</sup> and the TRO hearing<sup>6</sup>, held on September 29, 2006, this presumably was a result of the time necessary to wind down the affairs of RCM Biothane including the restoration of

---

<sup>5</sup>The disputed-as-to-effect Separation Agreement provides, "Biothane will cooperate fully with Moser to facilitate his ability to carry on his business going forward including the expeditious restoration of his computer system independent of Biothane's computer system and modification of the website to reflect and communicate with RCM Digesters." (Separation Agreement at 2.)

<sup>6</sup>At the TRO hearing, this Court ordered, "that, except as necessary to wind down the affairs of RCM Biothane, LLC, and except for the inadvertent use by defendants of the name 'Biothane' as a result of the parties' joint computer systems, defendants herein are preliminarily enjoined from using the 'Biothane' trademark." (Docket No. 6.)

separate computer systems.

In October 2006 through November 3, 2006 - after the parties' joint venture had ceased, after plaintiffs had sued in this Court to enforce that dissolution, and after this Court had granted their request for certain injunctive relief but while the computer systems were still connected for technical reasons - plaintiffs admit that they copied approximately 152,000 documents contained on defendants' cube server in Oakland.<sup>7</sup> They did so without any notice to this Court or their adversaries - an act both brazen and surreptitious at the same time.

Importantly, the documents copied included defendants' proprietary business information created after the dissolution of RCM Biothane, including contracts, grants, and designs. Defendants did not find out about plaintiffs' copying of their files, however, until a year later on October 18, 2007 during the deposition of Stephen Murphy, despite defendants' requests for documents ten months earlier. Following that revelation, defendants were granted leave to amend their counterclaims against plaintiffs to include claims pursuant to California Penal Code § 502, Computer Data Access and Fraud Act (Count 19), N.J.S.A. 2A:38A-1, Computer Related Offenses Act (Count 20), California Business & Professional Code § 17200, California Unfair Competition (Count 21), and for

---

<sup>7</sup>Moser severed the connection on November 3, 2006. At that point, he was not aware that plaintiffs had accessed the Oakland server and copied all files on it.

common law conversion (Count 22). Defendants also sought discovery violation sanctions against plaintiffs.

On June 27, 2008, Magistrate Judge Joel Schneider issued an Opinion and Order on defendants' motion for sanctions. Judge Schneider considered plaintiffs' explanation and justification for the file copying: (1) Moser was unresponsive to plaintiffs' proposed plan to sever the connection, and they copied the files in order to prevent a security risk if Moser were to disconnect the computers in an unsafe way; (2) Moser knew the computers were still connected, so he assumed the risk of his files being copied; (3) defense counsel sent plaintiffs a "litigation hold" letter on October 11, 2006, which imposed on them a duty to preserve all documents within their possession, custody or control; (4) plaintiffs owned the joint computer system, and therefore had the right to access anything on the network. (Op. at 9.) Judge Schneider then considered defendants' opposition to plaintiffs' proffered reasons: (1) plaintiffs' preservation excuse is an after-the-fact concoction to justify their illegal actions; (2) they deny plaintiffs' contention that they did not use the documents for litigation advantage; and (3) they deny plaintiffs' contention that they had a right to access defendants' cube server in Oakland. (Op. at 9-10.)

In the context of determining whether plaintiffs committed a discovery violation, and determining whether plaintiffs' complaint

should be dismissed for fraud on the court, Judge Schneider found that plaintiffs' conduct, while secretive, did not warrant the imposition of the ultimate penalty of the dismissal of their complaint because there was no evidence that plaintiffs' conduct was to obtain a litigation advantage. Instead, Judge Schneider found that plaintiffs' conduct was done for a business advantage. Judge Schneider also found, however, plaintiffs' conduct to be "troubling," and ordered plaintiffs to reimburse defendants for reasonable out-of-pocket costs defendants incurred, although not attorneys' fees. (Op. at 19.) Judge Schneider further commented that his ruling on the discovery issues did not prejudge defendants' legal claims.<sup>8</sup>

Based on essentially the same arguments and evidence advanced with regard to defendants' motion for discovery sanctions, both plaintiffs and defendants have moved for summary judgment in their favor on defendants' claims arising out of plaintiffs' copying of defendants' computer files. In defendants' motion, they state that they seek judgment in their favor on liability, and with regard to damages, they are only currently seeking equitable relief - namely, the return of all data and the enjoining of plaintiffs' use of that data - because the calculation of money damages is for the jury to

---

<sup>8</sup>As discussed below, Judge Schneider made findings with regard to several of plaintiffs' proffered justifications for copying defendants' computer files. His findings will be discussed in the context of the analysis of defendants' claims.

decide.<sup>9</sup> (Docket No. 181 at 30.)

The Court first turns to whether plaintiffs are liable substantively for defendants' four claims related to the file copying, each of which will be addressed in turn.<sup>10</sup> In this analysis, the Court will distinguish the copying of those documents that were created after August 7, 2006 from those that were created before. This distinction is necessary because the documents plaintiffs copied from defendants' computer server that were created after the August 7, 2006 business divorce are undisputably the sole property of defendants, while the right - or joint right - to the documents created prior to the dissolution of RCM Biothane is not as clear. The Court will then consider, in the context of damages, defendants' request for injunctive relief.

---

<sup>9</sup>Plaintiffs seek judgment in their favor on defendants' claims, but they state they "have no objection to returning all backed-up data." (Docket No. 186 at 15.) Plaintiffs make this overture in their reply brief in support of their motion for summary judgment. In an apparent change of tune in opposition to defendants' motion for summary judgment, plaintiffs argue that defendants are not entitled to the return of their copied files, because that would presume that they have succeeded on their claims. (Docket No. 193 at 20.) The Court will credit plaintiffs' offer to return the data, as modified below, and will accept that by that offer they are not conceding liability.

<sup>10</sup>Following the briefing of these motions, the parties filed a stipulation of dismissal as to Counts 19, 20, and 22 as to the individual defendants Martin Kaplan, Ron Kaplan, Graig Rosenberger, and Michael Holtz. (Docket No. 194.)



**1. Count 19 - California Penal Code § 502, Computer Data Access and Fraud Act**

Defendants claim that plaintiffs violated California Penal Code § 502(c), Computer Data Access and Fraud Act, when they secretly accessed and copied defendants' computer files.<sup>11</sup> Section 502(c) provides, in relevant part,

[A]ny person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. . . .

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or

---

<sup>11</sup>Neither party explicitly so states, but presumably because JOHI is a New Jersey corporation which accessed the computer files on a server located in California, the act of copying those files can be violative of both New Jersey and California law. See (Count 19) California Penal Code § 502(j) ("For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."); (Count 20) N.J.S.A. 2A:38A-6 ("Actions brought under this act may be filed in the Superior Court of the county in which the computer which is accessed is located, or where the terminal used in the accessing is situated, or where the actual damage occurs.").

computer network. . . .

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

West's Ann. Cal. Penal Code § 502(c). Thus, the primary issue with regard to most subsections of this statute is whether any disputed issue of material fact exists with regard to defendants' claim that plaintiffs "knowingly and without permission" accessed, and/or copied, and/or deleted defendants' computer files.<sup>12</sup>

**a. Liability**

Defendants have provided evidence that following the dissolution of RCM Biothane, and the filing of plaintiffs' instant lawsuit to enforce the Separation Agreement's terms of that dissolution, plaintiffs, without the knowledge or express permission of defendants, secretly accessed defendants' server located in Oakland, California and copied over 150,000 of defendants' files, many of which were created after the August 7, 2006 business divorce. Defendants have also provided evidence that plaintiffs called their actions the "Information Copy Project," and that they intended to keep it a secret, which they did for over a year. They have also provided evidence that computer desktop "shortcuts" were placed on the computers of the individual

---

<sup>12</sup>As discussed below, although there is substantial overlap, each of the 502(c) subsections has a distinct set of elements.

plaintiffs and other Biothane employees so that they would have quick access to the copied files. Defendants have provided evidence with regard to the deletion of files and changing of administrative passwords. Defendants have also provided evidence that at the time plaintiffs accessed the cube server, (1) it had reverted back to the property of RCM Digesters, (2) RCM Biothane, which previously had access to the cube server, was defunct, and (3) plaintiffs had no interest or rights in RCM Digesters.

Plaintiffs do not refute most of defendants' above proof. Plaintiffs, however, argue that they did not violate the California Penal Code because they had permission to access those computer files. Plaintiffs' professed permission is based on the theory that they were simply preserving evidence as instructed by defendants' "litigation hold" letter.<sup>13</sup> Specifically, on October 11, 2006, defendants' counsel sent plaintiffs a letter reminding them of their obligation to preserve electronic evidence, and instructing them to identify entities "currently or formerly associated with JOHI, Biothane Corporation, and/or RCM Biothane," and take "steps to ensure that all recorded information potentially relevant to JOHI's claims and defenses and any potential counterclaims or defenses that [defendants] might raise, wherever

---

<sup>13</sup>Plaintiffs go so far as to construe defendants' litigation hold letter to provide "clear authorization" by defense counsel to allow plaintiffs' access to defendants' server.

that material may be found, are identified and preserved pending resolution of this matter.” (Ex. G to Docket No. 170.) Further, plaintiffs represent that after receiving this letter, plaintiffs “were concerned that Moser would recklessly destroy electronic information by attempting to unilaterally sever the joint system,” so they “began to make a backup copy of the data that was on the joint server in Oakland.” (Pl. Br. at 5, Docket No. 170.) Additionally, plaintiffs state that because defendants and their attorneys knew the computers were still connected via the VPN, they should have expected plaintiffs to copy defendants’ files when they received defendants’ litigation hold letter. Thus, based on the litigation hold letter, and plaintiffs’ fears that Moser would usurp their duty to preserve by severing the connection, they permissibly accessed the server and began the Information Copy Project.

Plaintiffs’ theory, presented as a blanket shield to liability for all aspects of their “Information Copy Project,” has been rejected twice by Judge Schneider, and will be rejected again by this Court.<sup>14</sup> First, plaintiffs’ argument that their copying of

---

<sup>14</sup>In Judge Schneider’s March 27, 2008 Order granting defendants leave to file amended counterclaims based on the discovery of the Information Copy Project, he stated, “Plaintiffs do not cite any legal authority for their contention that their duty to preserve relevant documents immunizes them from liability for accessing a computer system owned by another party. Nor do plaintiffs point to any applicable ‘safe harbor’ provision in the statutes cited in defendants’ amended counterclaims.” (March 27,

defendants' computer files was solely based on their obligations under the Federal Rules to preserve evidence is belied by the secretive nature of the copying, as well as the creation of desktop shortcuts which ostensibly allowed plaintiffs to access the data. The duty to preserve evidence for litigation is just that--for preservation of documents as they existed at the commencement of litigation. Further, that duty is to preserve one's own documents. It is not to serve as a method by which to create an accessible database of an adversary's proprietary information.<sup>15</sup>

Second, an adversary's counsel's letter regarding the duty to preserve evidence does not afford a party carte blanche authority to secretively copy computer files located on the adversary's computer server. This is true even if many of those files on the server had once been property of that party, and even if that party still has access to those files. As analogized by defendants,

---

2008 Op. at 8.)

In Judge Schneider's June 28, 2008 Order on defendants' motion for discovery sanctions, he stated, "[T]he Court recognizes that no significant contemporaneous evidence has been submitted by plaintiffs to demonstrate that it copied defendants' documents in response to defendants' October 11, 2006, Litigation Hold Letter. This justification appears to this Court to have been proffered by plaintiffs' lawyer in its brief and in some recent deposition testimony of plaintiffs' witnesses." (June 28, 2008 Op. at 13.)

<sup>15</sup>It appears that plaintiffs were disgruntled by defendants' failure to comply with plaintiffs' "detailed, well thought-out presentation on how to disconnect the Oakland computer system from Joseph Oat Holdings computer system." (Pl. Br. at 8, Docket No. 193, Deposition of Jay Murphy.)

simply because plaintiffs had access through the network to defendants' server, they had no more authority to take those files than they would if they had a key to defendants' building, secretly entered it, and copied defendants' paper files.

If plaintiffs had been truly concerned about defendants' methods for severing the VPN connection and potentially destroying documents relevant to the litigation, they could have come to the Court for relief. Indeed, plaintiffs instituted the lawsuit against defendants with regard to the termination of their business arrangement, and sought and obtained a TRO to enforce the business divorce. Thus, plaintiffs had the means, inclination, and ability to again come to the Court to seek immediate assistance with their duty to preserve evidence. Because they did not do so, their explanation to justify the secretive copying of defendants' computer files is untenable.<sup>16</sup>

Plaintiffs also advance two other theories for why they should not be held liable for any wrongdoing with regard to their copying of the files off of defendants' server. First, plaintiffs argue that their conduct is protected by the litigation privilege. Second, plaintiffs argue that they "owned" the data, and therefore

---

<sup>16</sup>As Judge Schneider found in his June 28, 2008 Order on defendants' motion for discovery sanctions, "Plaintiffs' copying, which was done wholly independent of their lawyers was done to protect their business interests, not to gain a litigation advantage in this case." (June 28, 2008 Op. at 14.)

did not need permission to access it. The first argument is unavailing, and the second is, with regard to the documents created after August 7, 2006, patently false.

The litigation privilege grants an absolute privilege to statements or communications made by attorneys or litigants in the course of judicial and quasi-judicial proceedings. Component Hardware Group, Inc. v. Trine Rolled Moulding Corp., 2007 WL 2177667, \*5 (D.N.J. 2007) (citing Baglini v. Lauletta, 768 A.2d 825, 833 (N.J. Super. Ct. App. Div. 2001)). This privilege is "granted to good and bad alike," and it "promotes the unfettered expression that is critical to the administration of justice; [s]uch freedom would be defeated if participants in the process feared later tort liability." Hawkins v. Harris, 661 A.2d 284, 289 (N.J. 1995). Plaintiffs argue that "[c]ommon sense and fairness dictate that a litigant should be permitted to discharge their e-discovery duties without the fear of being subjected to additional causes of action." (Pl. Br. at 25, Docket No. 170.)

The Court agrees with that sentiment, but it is inapplicable here. As discussed, the Court has found that plaintiffs' clandestine copying of computer files was not conducted purely for litigation, or, more specifically, e-discovery purposes.<sup>17</sup>

---

<sup>17</sup>The question of whether the litigation privilege applies is a matter of law. Hawkins v. Harris, 661 A.2d 284, 289 (N.J. 1995).

Therefore, the litigation privilege is inapplicable.

With regard to plaintiffs' argument that it has an ownership interest in the data, and therefore plaintiffs cannot be liable for copying that data, that argument, even if credible, does not explain the copying of data created after the dissolution of RCM Biothane.<sup>18</sup> Issues of material fact remain as to the interpretation and effect of the Separation Agreement, and as discussed below, the future resolution of that issue may be dispositive to establishing the parties' rights to the defunct company's data, but there is no defense offered to plaintiffs' "knowing[ing] and without permission" accessing and copying defendant's post-dissolution computer files.<sup>19</sup>

---

<sup>18</sup>Plaintiffs also argue that the Court's Opinion denying plaintiffs' motion for summary judgment, in which the Court found that material issues of fact exist over whether the Separation Agreement was intended to be the final word on the parties' business divorce, leaves open the possibility that RCM Biothane was not dissolved on August 7, 2006, and if it was not, plaintiffs would still have an interest in all of the data. This argument misconstrues the Court's Opinion. As the Court noted, the one undisputed fact is that the parties agreed that RCM Biothane ceased to exist on August 7, 2006. Plaintiffs sought and obtained a TRO to enforce that split. It is the terms of the business divorce, and not the existence of the divorce, that is still in dispute.

<sup>19</sup>The Court notes that the dissolved entity RCM Biothane "owned" the copied computer files until August 7, 2006. The Separation Agreement addresses electronic documents twice: (1) "All documents received by [RCM Biothane] and its subsidiaries as part of the Asset Purchase Agreement are to be expeditiously returned to Moser or, in the case of electronic files, erased." and (2) "All documents and electronic files generated in pursuit of sales related to manure digestion shall be expeditiously



An alternative basis for judgment in plaintiffs' favor on this claim is defendants' inability to prove damages. Plaintiffs base their argument on the fact that defendants' alleged costs have been assessed to be general litigation expenses by Judge Schneider in the context of defendants' motion for sanctions for plaintiffs' discovery violations. Because plaintiffs' copying of the computer files was simply for discovery purposes, plaintiffs argue that defendants' costs relating to analyzing and copying that discovery are merely litigation expenses, and not damages for violations of the California Penal Code.<sup>20</sup>

This argument presumes, however, the validity of plaintiffs' preservation-of-documents justification. Since it has been determined that plaintiffs' file copying was not done simply for discovery purposes, plaintiffs' argument with regard to damages is without merit. Further, although defendants' analysis of the copy of the files produced by plaintiffs in discovery may be considered litigation expenses in the context of the exchange of discovery, the analysis of the copied files may be considered damages in the

---

provided to Moser." (Separation Agreement at 2.) Who "owned" the RCM Biothane files after its dissolution remains a disputed issue, however, because the effect and interpretation of Separation Agreement must be resolved by a jury.

<sup>20</sup>Plaintiffs advance this argument more generally as a basis for judgment in their favor on all of defendants' claims arising from the file copying. Even though the Court is addressing this argument in the specific context of Count 19, the Court also rejects this argument as to all other claims.

context of plaintiffs' liability for violations of the California Penal Code.<sup>21</sup>

Now that plaintiffs' bases for whether they had "permission" to access defendants' server have been rejected, it must be determined whether issues of material facts exist as to the elements of defendants' claim under California Penal Code § 502(c). Defendants have advanced claims under subparts (1), (2), (4), (6), and (7). The Court finds that no material issues of fact exist as to the documents created after August 7, 2006, but issues remain as to the pre-August 7, 2006 documents.

With regard to subpart (1), the statute requires in relevant part that defendants establish that plaintiffs "knowingly access[ed] and without permission . . . used" data from their computer server and did so with the intent to either "defraud, deceive, or extort" or "wrongfully control ... data." With regard to subpart (2), the statute merely requires that defendants establish that plaintiffs "knowingly access[ed] and without permission . . . copie[d]" data from their computer server. The distinction between the data created pre- and post-divorce is relevant here to these two subsections.

As to the data created after the August 7, 2006 split, no

---

<sup>21</sup>It is axiomatic that defendants would review the data surreptitiously copied by plaintiffs in order to assess what information plaintiffs had access to.

rational factfinder could conclude that plaintiffs had permission to copy the files of a completely separate and unrelated entity, and particularly a competitor. Likewise, a rational factfinder would have to conclude under subsection (1) that the unauthorized copying of a competitor's proprietary information was "wrongful" as defined by the statute and the California legislature.<sup>22</sup> Thus, we hold as a matter of law plaintiffs' conduct was clearly a violation of both subsections (1) and (2) of section 502(c) of the Computer Data Access and Fraud Act.

As to the data created during the life of RCM Biothane, a question arises as to whether plaintiffs required permission to access that data. As noted above, see supra note 19, it is unclear who owned the pre-divorce data after the split. The resolution of that issue centers around the interpretation and effect of the Separation Agreement, and that determination must be made by a jury. The resolution of that issue also must take into consideration that plaintiffs' and defendants' computer systems were still connected after August 7, 2006. At this point, the

---

<sup>22</sup>As the Court later holds, see infra pp. 25-26, plaintiffs' unauthorized copying of defendants' proprietary information, whether or not by computer, is a violation of California's unfair competition law and therefore by definition wrongful. See Iconix, Inc. v. Tokuda, 457 F. Supp. 2d 969, 997-98 (N.D. Cal. 2006) (noting complementary relationship between California's Computer Data Access and Fraud Act and Unfair Competition Law).

Court cannot conclude as a matter of law that plaintiffs did or did not have rights to that data, and therefore did or did not have "permission" to copy that data. Consequently, summary judgment in defendants' favor must be entered as to the post-August 7, 2006 data, but summary judgment must be denied as to either party as to the pre-August 7, 2006 data.

This same analysis applies to subparts (6) and (7), which requires defendants to show that plaintiffs "knowingly and without permission accesse[d]" the defendants' computer server or provided another the means to do so since after accessing the proprietary information plaintiffs shared the information among themselves and facilitated that sharing through computer shortcuts. Thus, there are no material issues of fact with regard to plaintiffs' violation of these subparts with regard to the post-August 7, 2006 data, but issues remain regarding the pre-August 7, 2006 data.

With regard to subpart (4), plaintiffs must show that defendants "knowingly access[ed] and without permission . . . alter[ed], damage[d], . . . or destroy[ed] any data." Plaintiffs dispute that they altered, damaged or destroyed any of defendants' data. Defendants present evidence, in a form of an email from plaintiffs' computer consultant, that he changed the administrative passwords to the server and also deleted his "monthly image backups." (Docket No. 179-9, Ex. 48.) Plaintiffs do not appear to dispute the changing of passwords, but they do dispute that the

computer consultant's erasing of his back-up image constituted a deletion of defendants' files. To the extent that the changing of defendants' passwords constitutes the "altering" of data, which plaintiffs do not appear to contest, plaintiffs have violated subpart (4). Disputed facts exist as to the effect of the deletion of the back-up image. The Court finds convincing, however, defendants' own expert, who states that the back-up image would only be implicated in a system failure. (Docket No. 170, Ex. Q at 9.) Thus, although the deletion of the back-up image may constitute a violation, because there was no system failure, defendants have proven no damages on this issue, and therefore, liability cannot be imposed on plaintiffs on this discrete act.

Based on the foregoing, the Court finds in favor of defendants as to plaintiffs' liability for Count 19 with regard to § 502(c), subparts 1, 2, 6 and 7 as to documents created after August 7, 2006. Summary judgment is denied as to these subparts as to documents created prior to August 7, 2006. Summary judgment is granted to defendants as to liability for subpart 4 with regard to password changes, but summary judgment is granted in favor of plaintiffs with regard to the deletion of the back-up images.

**b. Damages**

With regard to damages, the following are available for violations of § 502(c): (1) Compensatory damages, which includes "any expenditure reasonably and necessarily incurred by the owner

or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access"; (2) Injunctive relief; (3) Other equitable relief; and (4) Reasonable attorney's fees. West's Ann. Cal. Penal Code § 502(e). Section 502 also provides,

In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

Id.

Defendants seek all of these damages, but at this stage, they ask only for injunctive and equitable relief. As explained by this Court in a prior Opinion, issues left unresolved at summary judgment on these claims must be submitted to a jury. Therefore, it is up to a jury to decide the amount of damages defendants are entitled.<sup>23</sup>

With regard to injunctive and equitable relief, plaintiffs are

---

<sup>23</sup>Plaintiffs argue that it would be a burden on this Court and a jury for the issue of defendants' damages, totaling less than \$5,000, to go to a jury. Plaintiffs' assessment of compensatory damages, even if believed, does not account for the possibility the jury will award punitive or exemplary damages. Further, the amount of defendants' damages is not dispositive to the issue of whether damages must be presented to a jury. The Court notes that if plaintiffs are truly concerned about the burden this will place on the jury, they have the ability to settle this claim if they so desire, particularly now that liability has been imposed on them.

directed to return all the copies of the post-August 6, 2007 data obtained from defendants' server, and they are enjoined from using that data in any manner.<sup>24</sup> With regard to the pre-August 6, 2007 data, it appears that on December 5, 2007, plaintiffs produced what they represented to be an exact duplicate of the copied files. (Docket No. 177 at 14.) Because summary judgment is denied as to whether plaintiffs copied the pre-divorce data "without permission," no injunction will be issued with regard to that data.

## **2. Count 20 - N.J.S.A. 2A:38A-2**

Defendants have also advanced claims pursuant to the New Jersey's Computer-Related Offenses Act, N.J.S.A. 2A:38A-2(a), (c), and (e) for plaintiffs' copying of defendants' computer files. This Act provides, in relevant part,

A person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor in the Superior Court . . . :

a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment

---

<sup>24</sup>It is unclear to the Court exactly how plaintiffs have used that data, other than defendants' claims that plaintiffs have used it to compete with them and steal business away from them. The value of these damages is to be assessed by a jury. For the purposes of injunctive relief, because the Court has found that plaintiffs violated California Penal Code § 502(c) by copying the data, they are not entitled to use any information from that data. However, to the extent that plaintiffs had independent access to the data created prior to the August 7, 2006 split, the Court cannot enjoin the use of that information. This directive may be modified pending the resolution of the interpretation of the Separation Agreement.

existing internally or externally to a computer, computer system or computer network; . . .

c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network; . . .

e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

N.J.S.A. 2A:38A-3.

**a. Liability**

This Act mirrors the California Penal Code § 502(c), in that to violate the Act, a party must "knowingly and without authorization" access and/or take and/or alter another party's computer data. Therefore, for the same reasons above, summary judgment must be entered as to liability in defendants' favor with regard to subparts (c) and (a) for post-August 7, 2006 data. Summary judgment is denied as to these subparts for pre-August 7, 2006 data. With regard to subpart (e), summary judgment as to liability must be entered in defendants' favor as to the changing of passwords, but summary judgment must be entered in plaintiffs' favor as to the deletion of the back-up image.

**b. Damages**

As with the California Penal Code § 502(c), damages available under this Act include, "compensatory and punitive damages and the cost of the suit, including a reasonable attorney's fee, costs of



investigation and litigation.” N.J.S.A. 2A:38A-3. Damages for plaintiffs’ violation of this Act is an issue for a jury.<sup>25</sup> See N.J.S.A. 2A:38A-4 (“The value of damage, loss, property or income involved in any lawsuit shall be determined by the trier of fact.”). The same injunctive relief above will be imposed. See N.J.S.A. 2A:38A-5 (“In addition to any other action or proceeding authorized by law, the Attorney General, or a person or enterprise alleging injury or loss may bring an action in Superior Court to enjoin actions causing damage as described in this act or to enjoin any acts in furtherance thereof.”).

**3. Count 21 - California’s Unfair Competition Law - California Business & Professional Code § 17200**

Plaintiffs’ copying of the computer data also serves as a basis for defendants’ California Unfair Competition Law claim. Under that law, “unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division

---

<sup>25</sup>The Court notes that because each statute provides for compensatory and punitive damages, as opposed to a particular statutory fine, defendants cannot recover twice for the same conduct. See Midland Ins. Co. v. Colatrella, 490 A.2d 366, 370 (N.J. Super. Ct. App. Div. 1985) (noting the strong public policy against double recovery for the same injury or expense); 49 Prospect Street Tenants Ass'n v. Sheva Gardens, Inc., 547 A.2d 1134, 1151 (N.J. Super. Ct. App. Div. 1988) (noting that “since recovery on the various counts is based upon the same conduct by the defendants, there should be no double recoveries for economic loss”).

7 of the Business and Professions Code.” West's Ann. Cal. Bus. & Prof. Code § 17200. “Actions for relief pursuant to this chapter shall be prosecuted exclusively in a court of competent jurisdiction by . . . a person who has suffered injury in fact and has lost money or property as a result of the unfair competition.” Id. § 17204.

To maintain a claim under the UCL, a party must prove: (1) a violation “of almost any federal, state, or local law,” Plascencia v. Lending 1st Mortg., 583 F. Supp. 2d 1090, 1098 (N.D. Cal. 2008) (citation omitted),<sup>26</sup> and (2) that he has suffered an “injury in fact” and “lost money or property as a result of such unfair competition,” Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (citation omitted). Here, to the extent that plaintiffs seek summary judgment in their favor on this claim based on their same arguments advanced above, it will be denied. With regard to defendants’ motion for summary judgment, judgment must be entered in their favor as it pertains to plaintiffs’ unauthorized data copying because it has been established that plaintiffs have violated several laws and defendants have suffered an injury and lost money. The computation of damages is for the jury.

---

<sup>26</sup>A business practice may be “unfair or fraudulent in violation of the UCL even if the practice does not violate any law.” Plascencia, 583 F. Supp. 2d at 1098 (citation omitted).

#### 4. Count 22 - Conversion

Defendants also claim that plaintiffs' copying of the computer data constitutes the common law tort of conversion. In New Jersey,<sup>27</sup> conversion has been defined as "an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of an owner's rights." LaPlace v. Briere, 962 A.2d 1139, 1144 (N.J. Super. Ct. App. Div. 2009) (citations omitted). Conversion is an intentional tort in that the defendant must have intended "to exercise a dominion or control over the goods which is in fact inconsistent with the plaintiff's rights." Id. The defendant need not knowingly or intentionally act wrongfully for a conversion to occur. Id.

The mere use of the property of another without permission of the owner does not necessarily amount to conversion, however. Id. Where the "casual and harmless use" of the chattel of another involves "no defiance of the owner's right of dominion" over the chattel, then no conversion has occurred. Id. "The theory behind conversion is that the actor has exerted such a major and serious interference with the plaintiff's rights to the chattel that in essence the law will force a judicial sale of the chattel upon the defendant." Id.

In weighing the seriousness of the interference with the

---

<sup>27</sup>Plaintiffs do not dispute that New Jersey law applies to this claim.

owner's rights to the chattel to determine if a conversion has occurred, the following factors should be considered: (a) the extent and duration of the actor's exercise of dominion or control; (b) the actor's intent to assert a right in fact inconsistent with the other's right of control; (c) the actor's good faith; (d) the extent and duration of the resulting interference with the other's right of control; (e) the harm done to the chattel; (f) the inconvenience and expense caused to the other. Id. (citation omitted).

With regard to computer data and copyrighted material, two additional issues arise. First, intangible property cannot be the subject of a conversion claim. Slim CD, Inc. v. Heartland Payment Systems, Inc., 2007 WL 2459349, \*12 (D.N.J. Aug. 24, 2007) (dismissing conversion claim because there was no allegation that any tangible property was converted; instead, the only property at issue was intangible customer transaction data transmitted via computer) (citing K-Tronik N.A., Inc. v. Vossloh-Schwabe Matsushita, 2006 WL 1281291, \*3 (D.N.J. May 10, 2006) (holding that customer lists identifying customers, market information on customer purchases and sales prices, and customer service procedures did not constitute tangible property for purposes of a conversion claim); Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc., 210 F. Supp. 2d 552, 568 (D.N.J. 2002) (quoting Nimmer on Copyright for the proposition that "[t]he torts of conversion and trespass relate to interference with tangible rather than

intangible property...." 1 Nimmer on Copyright ¶ 1.01[B][1][I], at 1-41 (2001))). Second, and corresponding to the first point, the Copyright Act preempts state law conversion claims regarding copyrighted intangible property. Tegg Corp. v. Beckstrom Elec. Co., 2008 WL 5101358, \*16 (W.D. Pa. 2008) (citations omitted).

Here, even though it has been found that plaintiffs have no wholesale defense to their "unauthorized assumption" of defendants' data, and that plaintiffs altered the condition of defendants' data (namely, the changing of passwords), several issues remain unresolved that preclude the entry of summary judgment. First, it appears that defendants' computer data is comprised of both tangible property as well as intangible, possibly copyrighted, property. Defendants describe the copied files to consist of "RCM Digester's trade secrets, design documents, plans, specifications, drawings, and other proprietary business information, including more than 650 that RCM had created after August 7, 2006, and including correspondence between Mr. Moser and his counsel in this litigation, client lists and leads, pricing documents, confidential negotiations, contracts, accounting documents, designs, trade secret data, basis of design documents ("BODD"), drawings, and other intellectual proeprty created by Mr. Moser and his employees." (Def. Br., Docket No. 181-3, at 10.) Thus, without more information, the Court cannot determine which data may serve as a basis for a conversion claim. Further, it is unclear to what extent plaintiffs' copying of defendants' files caused to exclude

defendants of their ownership rights. It is undisputed that defendants still had access to their data despite plaintiffs' impermissible copying of some of it. Consequently, issues of material fact exist as to defendants' conversion claim that preclude the entry of judgment in any party's favor.

**5. Count 18 - Federal Computer Fraud and Abuse Act ("CFAA");  
Count 23 - Civil Conspiracy; Count 24 - Aiding and  
Abetting**

Based on plaintiffs' unauthorized copying of defendants' computer files, defendants have also advanced claims pursuant to the Federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq., and for common law civil conspiracy and aiding and abetting. Defendants have not moved for summary judgment on these claims. Plaintiffs, however, have moved for summary judgment in their favor on these claims based on the same arguments advanced with regard to Counts 19-22. For the same reasons expressed above, plaintiffs' arguments do not provide the basis for judgment in their favor as to Counts 18, 23, and 24.

**CONCLUSION**

Defendants' motion for partial summary judgment as to plaintiffs' liability is granted as to Count 19, § 502(c), subparts 1, 2, 6, and 7 as to documents created after August 7, 2006. Summary judgment is denied as to these subparts as to documents created prior to August 7, 2006. Summary judgment is granted to defendants as to liability for subpart 4 with regard to password changes, but summary judgment is granted in favor of plaintiffs

with regard to the deletion of the back-up images. Defendants' motion for partial summary judgment as to Count 20 is granted with regard to N.J.S.A. 2A:38A-2 subparts (a) and (c) for post-August 7, 2006 data. Summary judgment is denied as to these subparts for pre-August 7, 2006 data. With regard to subpart (e), summary judgment as to liability must be entered in defendants' favor as to the changing of passwords, but summary judgment must be entered in plaintiffs' favor as to the deletion of the back-up image. For Counts 19 and 20, plaintiffs are directed to return all the copies of the post-August 6, 2007 data obtained from defendants' server, and they are enjoined from using that data in any manner. Money damages are for the jury to decide. Defendants' motion for summary judgment as to Count 21 is granted. The computation of damages on that claim is for the jury.

Plaintiffs' motion for partial summary judgment as to Counts 18, 21, 22, 23, and 24 is denied, and defendants' motion as to Count 22 is also denied.

An appropriate order will be entered.

Date: October 14, 2009

At Camden, New Jersey

s/ Noel L. Hillman

NOEL L. HILLMAN, U.S.D.J.